GESTION DU CYBER RISQUE

COMMAND STRATEGY

A PROPOS DE COMMAND STRATEGY

Cabinet indépendant **spécialisé en Services Financiers** et **expert en gestion d'actifs**, Command Strategy possède une base clients diversifiée : Asset Managers, Assureurs, Asset Servicers, Banques, Organismes Gouvernementaux.

Fort de 20 ans d'expérience de ses cadres sur toute la chaîne du conseil, de l'analyse stratégique à l'implémentation, le cabinet propose une triple compétence en **Finance, SI et Gestion de projet.**

Sécurisant la réalisation de projets ambitieux de transformation, il propose également des **formations et des outils sur-mesure.**

LA GESTION DU CYBER RISQUE, UNE COMPONSANTE PAS SI NOUVELLE DU RISQUE OPÉRATIONNEL

Au cours des dernières années, la digitalisation des entreprises et l'externalisation des données ont fortement contribué à accroitre l'exposition des professionnels du monde de la finance au cyber risque. Même s'il a su investir dans des solutions de défense, le secteur financier demeure toujours une cible privilégiée des hackers.

Que l'on parle de perte de données sensibles (stratégiques ou clients), de fuite financière, d'espionnage, de crash ou de corruption de systèmes d'information (physique ou non), il est constaté que ces risques sont relativement proches des **risques opérationnels**. Autrefois cantonnés à une qualification de « risque humain », les risques opérationnels sont désormais identifiés et quantifiés depuis plusieurs années par les entreprises du secteur financier, au même titre que les risques financiers.

Si les technologies de défense diffèrent entre le cyber risque et les risques opérationnels traditionnels, la méthodologie de gestion des risques reste toutefois la même.

Command Strategy

METHODOLOGIE

01 CARTOGRAPHIER LES RISQUES

Par département, et lister les risques transverses ainsi que les risques intrinsèques à chaque direction/business line/processus métier/solution IT.

02 QUANTIFIER LES RISQUES

En se basant sur un historique de données toujours plus complet.

8 entreprises sur 10 touchées chaque année

2,25 M d'€ de pertes en moyenne pour les **GE françaises***

240 000 € de pertes en moyenne pour les **PME françaises****

L'exercice consiste à croiser distribution de fréquence et distribution de sévérité pour quantifier le risque, et ainsi être en mesure de prioriser les tâches dans les étapes de réduction des risques.

*Global State of Information Security
**https://www.maddyness.com/2018/04/11/la-cybersecurite-des-pme-nouvel-eldorado-des-assureurs/

03 RÉDUIRE LES RISQUES

En mettant en place des défenses technologiques adaptées ou en se couvrant via une assurance calibrée en fonction de l'étape précédente.
Plusieurs cabinets de conseil sont spécialisés dans ce domaine, et de nombreux assureurs continuent de se positionner sur cette thématique, perçue comme l'un des enjeux majeurs de demain.

04 GÉRER LES RISQUES

En sensibilisant les parties prenantes au cyber risque et en mettant en place des outils de reporting, afin d'identifier les éventuelles failles et d'affiner sans cesse les processus. Pour la gestion des risques, des professionnels proposent des solutions « clés en main », comme **IBM** via sa solution de **GRC OpenPages**, qui couvre l'intégralité des enjeux GRC. Via différents modules et des vues spécifiques selon l'utilisateur et son rôle hiérarchique, la solution permet de gérer les risques de façon transverse, et fournit des outils d'aide à la décision à la fois intuitifs et configurables.
La culture de la gestion du risque opérationnel est donc facilitée et n'apparait plus comme une contrainte. Elle reprend notamment sa place prépondérante pour les enjeux d'audit et de reporting à la hiérarchie. **IBM** a su capitaliser sur ses solutions technologiques pour fournir un logiciel flexible, configurable, et intégrable (Watson, Cognos, connecteurs Rest API). Son implémentation permet ainsi d'améliorer la productivité des équipes, avec notamment une **réduction de 30% du temps passé sur les audits**, et **une diminution jusqu'à 50% du temps de traitement des risques et du suivi de ces derniers.**

Au-delà de l'aspect technologique, la mise en place d'un processus de gestion du cyber risque peut être pertinent pour transformer son approche de la gestion des risques, en incluant et en sensibilisant tous les employés aux risques opérationnels. Le département IT étant aujourd'hui indéniablement transverse au sein des institutions financières, la gestion du risque cyber (et donc du risque opérationnel) l'est tout autant, rendant primordiale l'utilisation d'une solution GRC de premier ordre.